Sub a1

CLAIMS

1. A method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

2. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary; and

sending the encrypted session key to the intermediary.

3. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary;

signing the encrypted session key using a private key associated with the intermediary; and

sending the signed and encrypted session key to the intermediary.

4. A method as recited in claim 1, further comprising storing the data stream at the intermediary.

5. A method for inspecting an encrypted data stream being transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, the method comprising:

storing a public key from a public/private key pair associated with one of the endpoints at a key storage;

storing a public key from a public/private key pair associated with the intermediary at the key storage;

obtaining, at said one endpoint, the intermediary's public key from the key storage;

encrypting, at said one endpoint, the session key using the intermediary's public key to produce an encrypted session key;

encrypting, at said one endpoint, the encrypted session key using a private key from the public private key pair associated with said one endpoint to produce a signed encrypted session key;

passing the signed encrypted session key to the intermediary;

obtaining, at the intermediary, the one endpoint's public key from the key storage;

decrypting, at the intermediary, the signed encrypted session key using the one endpoint's public key to return the encrypted session key;

decrypting, at the intermediary, the encrypted session key using the intermediary's private key to return the session key; and

using the session key at the intermediary to decrypt the encrypted data stream.

6. In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for performing the method as recited in claim 5.

7. In a network system having an external client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a method executed at the firewall comprising:

receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client;

authenticating the digital signature as belonging to the internal client;

decrypting the session key; and

decrypting the encrypted data being exchanged between the internal and external clients using the session key.

8. A method as recited in claim 7, wherein the encrypted and signed session key is encrypted using a public key from a public/private key pair associated with the firewall, and the decrypting comprises decrypting the session key using a private key from the pubic/private key pair.

9. A method as recited in claim 7, further comprising inspecting the data in an unencrypted form.

10. A method as recited in claim 7, further comprising storing the data in an unencrypted form.

11. In a network system having an external client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a computer-readable medium resident at the firewall storing computer-executable instructions for performing method as recited in claim 7.

12. A network system comprising:

an internal client and an external client configured to communicate encrypted data over a network using virtual private network communication, the data being encrypted using a session key;

an intermediary having access to the encrypted data being communicated between the internal client and the external client;

the internal client being configured to securely transfer the session key to the intermediary; and

the intermediary being configured to decrypt the data using the session key and to inspect the data.

13. A network system as recited in claim 12, wherein the internal client encrypts the session key prior to sending it to the intermediary.

14. A network system as recited in claim 12, wherein the internal client encrypts and signs the session key prior to sending it to the intermediary.

15. A network system as recited in claim 12, wherein the intermediary stores the data in unencrypted form.

16. A software architecture for a network system having two endpoints that exchange encrypted data over a network and through an intermediary, the encrypted data being encrypted using a session key known to the endpoints, comprising:

endpoint-resident code to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and

intermediary-resident code to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session

key to decrypt the encrypted data as it is being exchanged between the two endpoints.

17. A software architecture as recited in claim 16, wherein intermediary-resident code inspects the data in unencrypted form.

18. A software architecture as recited in claim 16, wherein intermediary-resident code stores the data in unencrypted form.

19. In a network system having an external client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, computer-readable media distributed at the internal client and the firewall storing computer-executable instructions for:

encrypting the session key at the internal client;

signing the encrypted session key with a digital signature associated with the internal client;

passing the signed and encrypted session key to the intermediary;

authenticating, at the intermediary, the digital signature of the internal client;

decrypting the session key at the intermediary;

decrypting, at the intermediary, the encrypted data using the session key; and

inspecting the data in route between the internal and external clients.

20. ~~In~~ Apparatus a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.